AMENDMENTS TO THE CLAIMS:

This listing of claims replaces all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A ~~network~~ processor, comprising:

a crypto system;

an alignment buffer to receive header data and ciphered data from the crypto system, the crypto system encrypting data to form ciphered data so that an intended receiver with a correct cryptographic key may decrypt the ciphered data; and

a switch fabric having a plurality of transmit buffer elements to receive data from the alignment buffer, wherein the alignment buffer provides data to the switch fabric in blocks having a predetermined size.

2. (Currently Amended) The ~~network~~ processor according to claim 1, further including an interface to transmit data from the switch fabric.

3. (Currently Amended) The ~~network~~ processor according to claim 2, wherein the interface includes a SPI4 type interface.

4. (Currently Amended) The ~~network~~ processor according to claim 2, wherein the interface includes an NPSI interface.

5. (Currently Amended) The ~~network~~ processor according to claim 1, wherein the crypto system includes first and second crypto units.

6. (Currently Amended) The ~~network~~ processor according to claim 1, wherein the crypto system comprises ~~includes~~ a ~~predetermined number~~ plurality of crypto unit processing contexts and the alignment buffer comprises ~~includes~~ a number of buffer elements equal to a ~~element for each of the predetermined~~ number of processing contexts, and

wherein the plurality of processing contexts are configured to process at least one data packet at a time and to store cipher keys and algorithm context associated with processing the at least one data packet.

7. (Currently Amended) The ~~network~~ processor according to claim 1 ~~6~~, wherein the crypto system includes a plurality of cipher cores.

8. (Currently Amended) The ~~network~~ processor according to claim 7, wherein the plurality of cipher cores correspond to a plurality of cipher algorithms.

9. (Previously Presented) A method of processing data in a device having at least one crypto unit, comprising:

storing a portion of a packet header in an alignment buffer that has a first storage size;

storing a first portion of a first data block of ciphered data from the at least one crypto unit in the alignment buffer, the at least one crypto unit encrypting data to form the ciphered data so that an intended receiver with a correct cryptographic key may decrypt the ciphered data;

transmitting the ciphered data from the alignment buffer to a first buffer element in a switch fabric interface unit;

transmitting further data blocks of the ciphered data from the alignment buffer to the first buffer element until the first buffer element is full;

allocating a second buffer element in the switch fabric interface unit; and

transmitting the ciphered data in the alignment buffer to the second buffer element.

10. (Previously Presented) The method according to claim 9, further including transmitting the ciphered data from the at least one crypto unit to a selected one of a plurality of elements in the alignment buffer.

11. (Original) The method according to claim 9, wherein the alignment buffer includes a number of buffer elements corresponding to a number of processing contexts for the at least one crypto unit.

12. (Previously Presented) The method according to claim 9, further including transmitting the ciphered data from the switch fabric interface unit over an interface.

13. (Previously Presented) The method according to claim 12, further including transmitting the ciphered data from the switch fabric interface unit over an SPI4 interface.

14. (Previously Presented) The method according to claim 9, further including transmitting the ciphered data from the switch fabric interface unit over an NPSI interface.

15. (Previously Presented) The method according to claim 9, further including transmitting the ciphered data from the alignment buffer in an amount that is a multiple of a predetermined number of bytes.

16. (Original) The method according to claim 15, wherein the predetermined number of bytes is 16.

17. (Previously Presented) The method according to claim 9, further comprising transmitting the ciphered data to the second buffer element in an amount less than the predetermined number of bytes for an end of packet.

18. (Previously Presented) A processor disposed on an integrated circuit, comprising:

first and second crypto units each having a plurality of cipher cores and a predetermined number of processing contexts, the first and second crypto units encrypting data to form ciphered data so that an intended receiver with a correct cryptographic key may decrypt the ciphered data;

an alignment buffer having a respective element for each of the plurality of processing contexts to receive the ciphered data from the first and second crypto units;

a switch fabric interface unit having a plurality of transmit buffer elements to receive the ciphered data from the alignment buffer in an amount that is a multiple of a predetermined number of bytes; and

an interface to transmit the ciphered data from the switch fabric.

19. (Previously Presented) The processor according to claim 18, wherein the interface includes an SPI4 interface.

20. (Previously Presented) The processor according to claim 18, wherein the interface includes an NPSI interface.

21. (Currently Amended) A network switching device, comprising:

a processor disposed on an integrated circuit comprising:

a crypto system, the crypto system encrypting data to form ciphered data so that an intended receiver with a correct cryptographic key may decrypt the ciphered data, the crypto system comprises ~~includes~~ a plurality ~~predetermined number~~ of crypto unit

processing contexts and the alignment buffer comprises ~~includes~~ a number of buffer elements equal to a ~~element for each of the predetermined~~ number of processing contexts;

an alignment buffer to receive header data and the ciphered data from the crypto system; and

a switch fabric interface unit having a plurality of transmit buffer elements to receive the ciphered data from the alignment buffer, wherein the alignment buffer provides the ciphered data to the switch fabric in blocks having a predetermined size,

wherein the plurality of processing contexts are configured to process at least one data packet at a time and to store cipher keys and algorithm context associated with processing the at least one data packet.

22. (Cancelled)

23. (Original) The device according to claim 21, wherein the crypto system includes a plurality of cipher cores,

wherein the plurality of cipher cores correspond to a plurality of cipher algorithms.

24. (Original) The device according to claim 21, wherein the device includes a router.

25. (Previously Presented) A network, comprising:

a network switching device including a processor disposed on an integrated circuit comprising:

a crypto system, the crypto system encrypting data to form ciphered data so that an intended receiver with a correct cryptographic key may decrypt the ciphered data;

an alignment buffer to receive header data and the ciphered data from the crypto system; and

a switch fabric interface unit having a plurality of transmit buffer elements to receive the ciphered data from the alignment buffer, wherein the alignment buffer provides the ciphered data to the switch fabric in blocks having a predetermined size.

26. (Currently Amended) The network according to claim 25, wherein the crypto system comprises ~~includes~~ a ~~predetermined number~~ plurality of crypto unit processing contexts and the alignment buffer comprises ~~includes~~ a number of buffer elements equal to a ~~element for each of the predetermined~~ number of processing contexts, and

wherein the plurality of processing contexts are configured to process at least one data packet at a time and to store cipher keys and algorithm context associated with processing the at least one data packet.

27. (Original) The network according to claim 26, wherein the crypto system includes a plurality of cipher cores.

28. (Original) The network according to claim 25, wherein the network switching device corresponds to a router.

29. (New) The processor of claim 6 wherein the plurality of processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the plurality of processing contexts with processing of the packet data in a second portion of the plurality of processing contexts.